CHAPTER 18

INTELLIGENCE ORGANIZATION AND MANAGEMENT

"No combat commander has ever had as full and complete a view of his adversary as did our field commander. Intelligence support to Operations DESERT SHIELD and DESERT STORM was a success story."

General Colin Powell, Chairman, JCS
1991

INTRODUCTION

The current National Military Strategy delineates a regional conflict emphasis—a marked change from a 40-year focus on the threat from the former Soviet Union. This emphasis and additional changes to national priorities are not only having a major impact on force structure, but also are changing the requirements for intelligence. As a result, continual changes in intelligence organizations and functions are occurring within the Army. As these occur, they will be outlined in future editions of this text.

This chapter defines intelligence and provides an overview of the need for intelligence by decision makers. It includes the composition and responsibilities of the various intelligence organizations at national, Department of Defense (DOD), non-DOD, and Service (including HQDA) levels. It describes intelligence as a fundamental support tool in the emerging doctrine of Information Operations. It also describes the Army concepts for management of all-source intelligence, or providing intelligence support to commanders; Operations Security support; targeting support; Electronic Warfare at the operational and tactical levels of combat; and the need for effective national-tactical intelligence interface.

Intelligence is the product obtained from the systematic collection, processing, analysis, production, dissemination, and assessment of available information on virtually any topic, area, or individual. This chapter addresses the management of this effort.

President Reagan signed *Executive Order (EO) 12333* on 4 December 1981. The *EO* provides for the effective conduct of U.S. intelligence activities and the protection of the constitutional rights of U.S. citizens. *EO 12333* superseded *EO 12036*, which regulated U.S. intelligence activities during the Carter Administration. The original *Executive Order* on the subject was *11905*, signed by President Ford. EO 12333 has not

been superseded under the current Administration.

NEED FOR INTELLIGENCE

Timely, relevant, accurate and synchronized information addressing the activities, capabilities, plans, and intentions of foreign leaders and their governments is needed to develop sound national security and foreign policies. It is critical to international negotiations and to the development and monitoring of international agreements. Within the DOD, planners and managers responsible for the development of weapons systems and force structure need accurate, long-range projections of the combat capabilities and technologies of foreign powers as the basis for their recommendations and decisions. The ability of U.S. forces to deter or defend against attack requires detailed knowledge of the current deployment and capabilities of potential adversaries and their future plans. At the operational and tactical levels of warfare, intelligence must provide a commander with an accurate picture of the battle space so that he can position and employ his forces successfully to accomplish the assigned mission. It is a key component of battle command and will provide the enemy portion of battle space awareness to the commander and his staff. Finally, as our focus shifts to additional missions, forces involved in small scale contingencies will require detailed information on the cultural, historical, economical, technological, and political milieu of the area in which they will deploy. Intelligence support to force projection operations will require a tremendous amount of information to ensure mission accomplishment with minimal casualties and limited collateral damage.

INTELLIGENCE PRODUCTS

Intelligence products may be categorized in several ways depending on the needs of the intended recipients as well as the scope, level of detail, and the perishability of the product. The distinctions between these types of intelligence products are becoming less pronounced as the nature of conflict, peacekeeping operations, and humanitarian assistance overlap. Additionally, technology facilitates the development, acquisition, and integration of all-source intelligence through a "seamless" architecture from the national to the tactical levels. Examples include the U.S. Army's All Source Analysis System (ASAS), the Joint Worldwide Intelligence Communications System (JWICS), the Joint Deployable Intelligence Support System (JDISS), NSA's interactive geographic database (OILSTOCK), and other similar types of multi-dimensional systems and capabilities.

Categories.

National Intelligence is integrated departmental intelligence coordinated by the National Foreign Intelligence Board (NFIB) and approved by the Director of Central Intelligence (DCI). It covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency.

Departmental Intelligence is intelligence that any department or agency of the Federal Government requires to execute its own mission. This may include any or all of the following: National Security Council (NSC) Staff, Central Intelligence Agency (CIA), Department of State and its

Intelligence and Research (I&R) staff, Department of the Treasury (Secret Service and the Bureau of Alcohol, Tobacco, and Firearms [BATF], Department of Justice (Federal Bureau of Investigation [FBI]), Department of Transportation (U.S. Coast Guard [USCG]); the National Drug Enforcement Office; and the DOD and its agencies to include the Defense Intelligence Agency (DIA), National Security Agency (NSA), National Imagery and Mapping Agency (NIMA), National Reconnaissance Office, and the Armed Forces.

Levels.

Strategic Intelligence is intelligence required for the formulation of strategy, policy, and military plans and operations at theater and above.

Operational Intelligence is the intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations.

Tactical Intelligence is intelligence required for planning and conducting tactical operations.

Types of Intelligence.

Basic Intelligence is encyclopedic type information which is not time-sensitive and describes all aspects of a nation — physical, social, economic, political, geographical, cultural, and military — which is used as a base for intelligence products in support of planning, policymaking, and military operations.

Current Intelligence includes all types and forms of perishable, time-sensitive, information of immediate value and interest to specific consumers. It may be disseminated without complete evaluation, interpretation, analyses, or integration.

Estimative Intelligence is that intelligence which projects forward in time and is predictive in nature.

Crisis Intelligence is comprised of specific types and forms of very perishable, time-sensitive information of immediate value, and usually intense interest at the international, national, and theater levels. It is narrowly focused on a precise area, individual(s), or event which is closely monitored until termination or closure. Usually after 30 days, this type of intelligence becomes Current Intelligence and eventually Basic Intelligence.

Combat Information is data obtained through intelligence collection sources and methods which are passed rapidly to the user without benefit of analysis, interpretation, or integration. A sensor-to-shooter system transmitting highly perishable, potential targeting data, is an example of this data. Tactical commanders often must make decisions based on the immediate access to and availability of combat information.

INTELLIGENCE DISCIPLINES

Intelligence is categorized by a series of interdependent disciplines. No single discipline can normally satisfy the commander's requirements. The actual mix of disciplines tasked to satisfy a requirement is situation dependent.

Human Intelligence (HUMINT).

HUMINT is a category of intelligence derived from information

collected and provided by human sources (Joint Pub 1-02) as opposed to technical sources. HUMINT includes such overt activities as attaché duty, liaison functions, interrogation of POWs, debriefing of displaced persons/refugees/evacuees/and line crossers, solicitation of information from indigenous persons, document exploitation, and controlled collection operations such as clandestine operations.

Imagery Intelligence (IMINT).

IMINT is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media (Joint Pub 1-02). The resulting imagery may be analyzed in either hard-copy (photographic) or soft-copy (electronic display) format for distribution.

Signals Intelligence (SIGINT).

SIGINT is intelligence obtained through the exploitation and analysis of electromagnetic emissions and includes Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

Measurement and Signature Intelligence (MASINT).

MASINT is that scientific and technical intelligence which is directed toward the identification of remotely-sensed, distinctive characteristics of a device or system which can facilitate subsequent identification. It plays a significant role in theater missile defense. It includes UAV video and JSTARS moving target indicators.

Technical Intelligence (TECHINT).

TECHINT is a multidiscipline function which supports commanders by either identifying or countering an enemy's momentary technological advantage, or by maintaining a friendly technological advantage. The two parts of TECHINT are Battlefield TECHINT and Scientific and Technical Intelligence (S&TI)

Counterintelligence (CI).

Counterintelligence is that intelligence which deals with the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, subversion, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or terrorist activities. Operations Security (OPSEC) Support, a subset of command and control (C2) Force Protection, is the counterintelligence assessment of the vulnerability of specific U.S. forces, areas, or activities to foreign intelligence collection.

Open Source Intelligence (OSINT).

Open source intelligence is intelligence derived from the collection and analysis of information which is unclassified and largely in the public domain. Open source intelligence may cut across other disciplines to include broadcast, imagery and mixed media sources.

OTHER USES OF INTELLIGENCE

Intelligence must quickly reach, or be accessible, to leaders and their staffs who require it in the preparation of plans and

orders. Commanders, J2s/G2s/N2s, action officers, and managers must develop a broad understanding of what intelligence they need; what can be reasonably obtained; and how it can be beneficial in the development of their programs. They must clearly state, and if possible, prioritize their intelligence requirements to the appropriate organization.

The following are a few examples of program areas in which intelligence can have a significant impact.

Organizational Design and Force Structure.

Force structure designers must consider the multiplicity of the threats and must also include nonthreat factors such as the deployment capabilities and limitations of allied forces. There must also be balance between the greatest threat or enemy capability and the most imminent threat or intention in the development of a force structure. The force planner must include intelligence participation in every phase of his planning and decision making. To do this, he must be aware of the intelligence support available and how to task the system.

Materiel Acquisition and Force Modernization.

The product/project/program manager must consider technical developments in foreign countries, new foreign weapons systems and countermeasures developments and future developments, as well as terrain and weather considerations. This includes an assessment of how an adversary may react to the development of a new, friendly system. The adversary reaction may include development of a totally new piece of equipment to counter a specific threat. The project manager must have the latest intelligence available which could affect his program. He must make the intelligence systems aware of his intelligence needs.

The combat developer must also be aware of technical developments and must work closely with the materiel developer to ensure that a project/program will counter or surpass assessed threat capabilities. Both must be prepared to amend a program prior to its completion to counter a new threat capability. Intelligence requirements are not limited to hostile forces.

Technological breakthroughs in friendly or neutral nations must also be factored into U.S. materiel acquisition planning. Managers of systems of breakthrough technology must use available intelligence support to protect characteristics of the developing system as a measure of OPSEC in the R&D arena.

In addition to the intelligence needs stated, the program/project/product manager must also have high quality up-to-date intelligence on the foreign collection threat directed at his program/project/product. Threats from both foreign government and non-government sponsored collection make up this category. These threats must be identified, collected against, and neutralized by Army Counterintelligence assets on behalf of the materiel developer. It is important to keep the Army materiel development community continually aware of and safe from technological loss from foreign directed and controlled collection services. This strengthens the Army's technical base against illegal technology transfer and markedly improves the Army's ability to maintain technological superiority.

Other factors that should be taken into account in these processes include long-range planning and consideration of opponent's strengths, weaknesses, and vulnerabilities. As the rate of technological growth continues to increase and as the threat becomes harder to define, material

developers lean toward generic threats defined in technical terms, thereby avoiding the potential trap of being locked to a specific adversary or region.

Training Systems Development.

Doctrine and training decisions must be based on sound intelligence. Foreign military capabilities and deployments are dynamic, and U.S. doctrine and training decisions must be equally dynamic. To be effective in battle, U.S. soldiers must know the enemy, including his doctrine, tactics, equipment, strengths, weaknesses, and vulnerabilities, and if possible, his intentions. Training development and implementation must be closely tied to materiel systems management. Training to operate in a hostile information warfare environment anywhere in the world places a heavy emphasis on learning about a broad range of technical command and control capabilities. Future adversaries may employ combinations of hostile, friendly, and neutral command and control systems, as well as commercial products.

THE NATIONAL FOREIGN INTELLIGENCE SYSTEM

The goal of the U.S. intelligence effort is to provide the President and the National Security Council information on which to base decisions concerning the development and conduct of foreign, defense, and economic policy, and the protection of U.S. interests from foreign threats. To reach this goal, the intelligence system is organized as shown at Figure 18-1. While not a member of the Intelligence Community (IC), the Office of Management and Budget (OMB) provides program and budget guidance to the Director of Central Intelligence for development of the National Foreign Intelligence Program (NFIP) as part of the Federal Budget.

Composition of the NFIP.

The NFIP provides funds for the bulk of all national-level intelligence, counterintelligence, and reconnaissance activities of the CIA, Defense Department, and all civilian federal agencies and departments, as well as the Intelligence Community management structure. The program is comprised of two major components - national level intelligence programs within the Defense Department and those in federal departments and agencies outside DOD. The Defense programs include the General Defense Intelligence Program (GDIP), the Consolidated Cryptologic Intelligence Program (CCP), The DOD Foreign Counterintelligence Program (FCIP), the National Imagery and Mapping Agency Program (NIMAP), the National Reconnaissance Program (NRP), and specialized DOD Reconnaissance Activities. The Program Manager for the GDIP is the Director, DIA; Program Manager for the CCP is the Director, NSA; Program Manger for the FCIP is the Director of Counterintelligence and Security Programs who is subordinate to the Deputy Assistant Secretary of Defense for Intelligence and Security, under the ASD (C3I); Program Manager for the NIMAP is the Director, NIMA, Program Manager for the NRP is the Director, National Reconnaissance Office (NRO).

Tactical Intelligence and Related Activities (TIARA).

TIARA accounts provide funding for timely intelligence support primarily to tactical operations of military forces. The

ORGANIZATION OF
THE NATIONAL FOREIGN INTELLIGENCE SYSTEM UNDER EO 12333

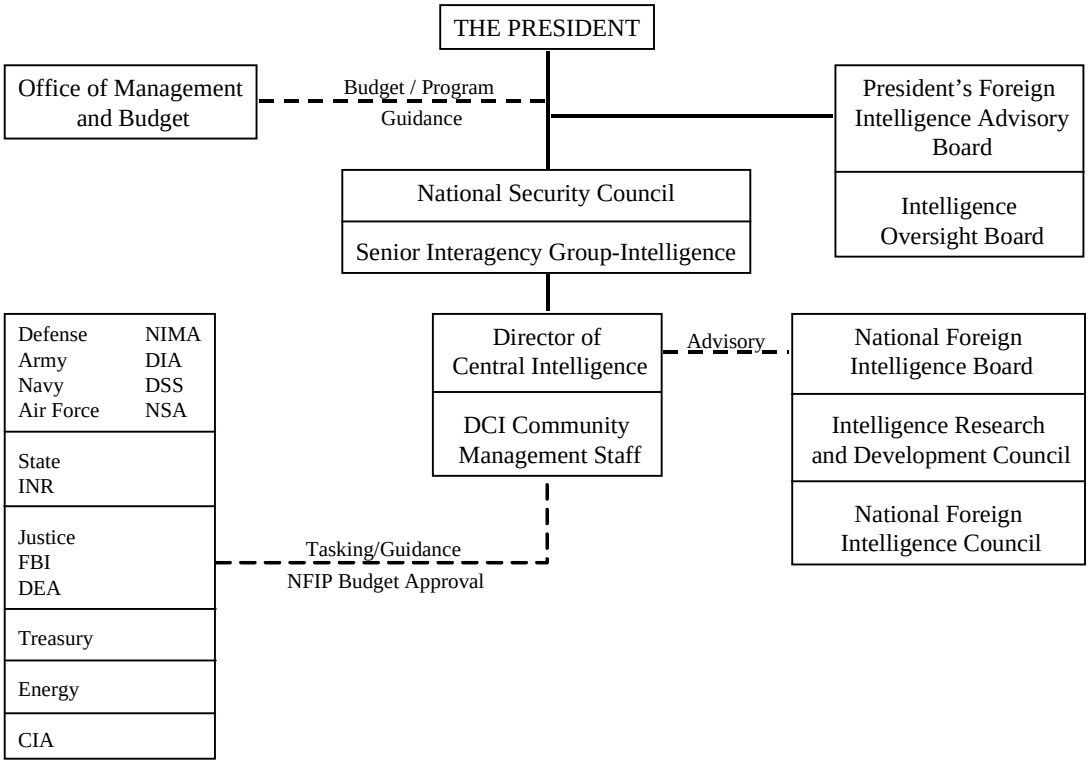

Figure 18-1

TIARA accounts are designed, built and operated by the military Services and defense agencies and compete for funding with the combat and combat-support programs they support. As defined by the Congress, TIARA funds represent those portions of the DOD budget devoted to activities outside the NFIP. TIARA is an aggregation of all portions of the DOD budget that provide intelligence and related support to military operations. In contrast to the NFIP, the TIARA assets are managed by countless military commanders and defense agency officials on a decentralized basis. The single DOD focal point for intelligence management is the ASD (C3I).

Joint Military Intelligence Program (JMIP).

The JMIP focuses on joint, defense-wide initiatives, activities and programs that predominantly provide intelligence information and support to multiple defense consumers; bridge existing programmatic divisions across Service, departmental and national intelligence lines to provide more effective and coherent intelligence programmatic decisionmaking; and ultimately support military intelligence consumers, i.e. warfighters, policymakers, and force modernization planners. JMIP encompasses the Defense Cryptologic Program (DCP), Defense Imagery and Mapping Program (DIMP), the Defense Mapping, Charting and Geodesy Program (DMC & GP), and the General Defense Intelligence and Applications Program (GDIAP).

The President's Foreign Intelligence Advisory Board (PFIAB).

The PFIAB reports directly to the President and advises him concerning the objectives, conduct, management and coordination of the various activities of the agencies of the Intelligence Community. In addition to the President, the DCI, the CIA, or other Government agencies engaged in intelligence activities can request PFIAB recommendations concerning ways to achieve increased effectiveness in meeting national intelligence needs.

By *Executive Order 12863*, September 13, 1993, the Intelligence Oversight Board (IOB) was established as a standing committee of the PFIAB. The IOB is required to report through the PFIAB to inform the President of intelligence activities that any member of the Board believes are in violation of the Constitution or laws of the United States, Executive Orders, or Presidential directives; to forward to the Attorney General reports received concerning intelligence activities that the Board believes may be unlawful; to review the internal guidelines of each agency within the Intelligence Community concerning the lawfulness of intelligence activities; to review the practices and procedures of the Inspectors General and General Counsel of the Intelligence Community for discovering and reporting intelligence activities that may be unlawful or contrary to an Executive Order or Presidential directive; and to conduct such investigations as the Board deems necessary to carry out its functions under this order.

The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).

The SSCI and HPSCI have key roles in the conduct of Intelligence Oversight. These roles, specified by law, require that the committees be kept fully and currently informed of all intelligence activities which are the responsibility of, are engaged in by, or are carried out for or on behalf of any department; that they be furnished any information or material concerning intelligence activities requested in order to carry out authorized responsibilities; and that the committees be informed in a timely fashion of any illegal intelligence activity or significant intelligence failure and any corrective action.

Within the Department of Defense the officer responsible for the oversight of intelligence activities is the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO). *DOD Directive 5148.12*, dated 20 July 1989, established the position and assigned its responsibilities. The ATSD-IO had been designated as the sole conduit between the Department of Defense and the President's Intelligence Oversight Board. In addition, the Assistant to the President for National Security Affairs is the coordinator of the National Security Council Staff and the senior executive officer for national security issues.

The National Security Council (NSC).

The NSC reviews, guides, and directs the conduct of all national foreign intelligence, counterintelligence, special activities, and attendant policies and programs. Within the NSC, the Senior Interagency Group - Intelligence formulates policy, monitors decisions, and evaluates the

adequacy and effectiveness of collection efforts.

The Director of Central Intelligence (DCI).

The DCI is concurrently Director, CIA, and is directly responsible to the President and the National Security Council. He is the primary adviser to the President and the NSC on national foreign intelligence and is the intelligence system's principal spokesman to Congress. He develops objectives and prepares guidance for the IC to enhance its capabilities for responding to expected future needs for foreign national intelligence, formulates policies concerning intelligence arrangements with foreign governments, and coordinates intelligence arrangements between agencies of the IC and the intelligence or internal security services of foreign governments. The DCI is responsible for the development, presentation, and justification of the National Foreign Intelligence Program budget. A complete list of DCI responsibilities is contained in *EO 12333*.

Other senior officials are responsible for contributing, within their areas of capability, to the national foreign intelligence collection effort and for cooperating with other IC members to achieve efficiency and provide mutual assistance. In addition, they are responsible for management of the collection of departmental intelligence.

Pursuant to *EO 12333*, the DCI establishes boards, councils, committees, or groups as required for the purpose of obtaining advice from within the Intelligence Community. Three such organizations are shown on Figure 18-1.

The National Foreign Intelligence Board (NFIB*).*

The NFIB advises the DCI on production, review, and coordination of foreign national intelligence; interagency exchanges of foreign intelligence information; arrangements with foreign governments on intelligence matters; protection of intelligence sources and methods; activities of common concern; and other matters referred to it by the DCI. Although not mentioned in *EO 12333*, the DCI continued the NFIB but removed from its charter responsibility for addressing resource issues. Those responsibilities were assigned to the National Foreign Intelligence Council.

The National Foreign Intelligence Council (NFIC).

The NFIC advises the DCI on priorities and objectives for the National Foreign Intelligence Program budget and any other such matters referred to it by the DCI.

Intelligence Research and Development Council (IR&DC).

The IR&DC advises the DCI on research and development strategy and technologies that will best contribute to the attainment of national intelligence objectives.

CIA responsibilities, under the direction of the NSC, include the collection of foreign intelligence and the development, conduct, or provision of support for technical and other programs which collect national foreign intelligence. The CIA is responsible for the conduct of counterintelligence activities conducted abroad by other members of the IC. In

contrast, the FBI is responsible for domestic counterintelligence activities. The CIA is also responsible for coordinating collection of intelligence information outside the United States. The CIA conducts special activities approved by the President and conducts services of common concern for the IC as directed by the NSC. Special activities are defined in *EO 12333* as: *activities in support of national foreign policy objectives abroad which are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly, and functions in support of such activities but which are not intended to influence U.S. political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.*

The CIA produces and disseminates foreign intelligence relating to the national security, including foreign political, economic, scientific, technical, military, geographic, and sociological intelligence required to meet the needs of the President, the NSC, and other elements of the U.S. Government. The CIA also produces and disseminates counterintelligence studies and reports on the foreign aspects of narcotics production and trafficking.

Recently established in the CIA is the Office of Military Support (OMS). The OMS provides a single point of contact to the military departments to facilitate coordination with the CIA.

The responsibilities of all agencies depicted in Figure 18-2 are detailed in *EO 12333*.

THE MANAGEMENT OF INTELLIGENCE

The National Security Council provides overall Executive Branch guidance, direction, and review for all national foreign intelligence and counterintelligence activities. The NSC has special committees within its framework, which deal with its intelligence responsibilities.

In addition to the management of the individual agencies or elements thereof which constitute the intelligence system, management of intelligence focuses mainly on intelligence resources, requirements, collection-tasking, collection, analysis, production and dissemination.

DEFENSE INTELLIGENCE

The DOD is the nation's largest user of intelligence information and the largest investor in intelligence programs. DOD has a particular responsibility to support commanders at all levels. Defense Intelligence, as part of the Intelligence Community (IC), is faced with a growing number of challenges to the successful accomplishment of its Defense intelligence mission.

The international environment has grown more complex. Changing political alignments and instability, growing economic interdependence, nationalistic tendencies and ethnic rivalries, increased international terrorism and transnational threats, international narcotics trade, *et al.* have resulted in more diverse intelligence requirements. A significant challenge is presented by trying to attack targets protected by relatively sophisticated command, control and communications systems which are readily available to even the poorest countries

Effective performance of Department of Defense missions depends upon the collection, analysis, production, and dissemination of timely, relevant, accurate, synchronized, and predictive intelligence on

DEFENSE INTELLIGENCE ORGANIZATION

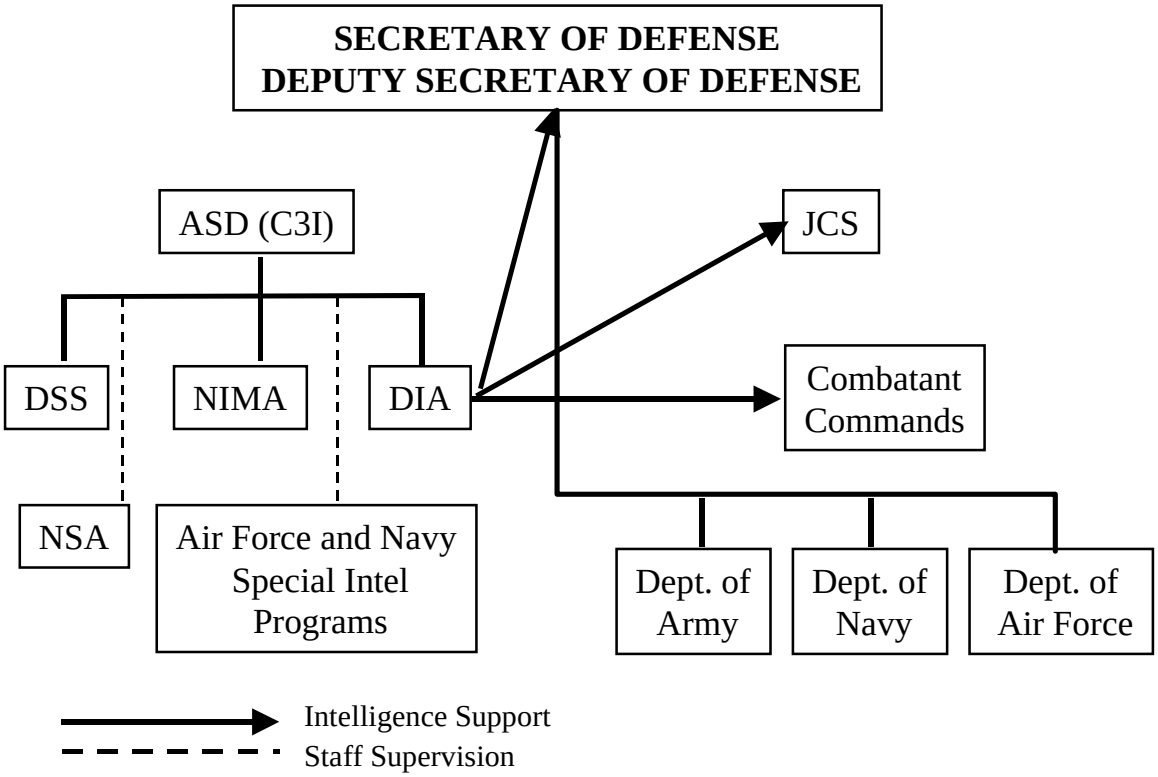

Figure 18-2

the capabilities and intentions of foreign powers.

To strengthen the Department's performance of its intelligence functions, on 15 March 1991 the Secretary of Defense approved a plan for restructuring Defense Intelligence. The DOD reorganization of Defense intelligence resulted in a structure to:

- Ensure the quality, relevance, and timeliness of defense intelligence in support of national and international defense and foreign policies, plans, and programs through establishment of a Defense Intelligence Policy Council to assist the ASD (C3I) and the IC.
- Strengthen the intelligence support to the Combatant Commanders and enhance "jointness" through consolidation of existing Unified and Major or Joint Combatant Commands and component intelligence processing, analysis, and production activities into Joint Intelligence Centers (JICs); reshape the CINC and Service component staffs into small, high quality groups that can provide focused intelligence evaluation support to the Combatant Commander; establish dedicated elements within DIA and to serve as a focus for all intelligence activities supporting the Office of the Secretary of Defense (OSD) and the Chairman, Joint Chiefs of Staff (JCS).
- Increase efficiency in Defense Intelligence by consolidating and streamlining to eliminate

unnecessary duplication and enhance efficiency and effectiveness through reduction of management overhead; reduction of overseas operating locations; consolidation of the various intelligence commands, agencies, and elements into a single intelligence command/agency within each Service; reduction of subordinate Service and Agency intelligence headquarters while maintaining intelligence production centers of excellence; establishment of stronger management of all Defense Intelligence production to eliminate overlap and unnecessary duplication; establishment of joint Regional SIGINT Operations Centers (RSOCs); zero-based review and reordering of Defense Intelligence requirements to reflect a worldwide, rather than a Soviet/Warsaw Pact focus; and examination of the centralization of order of battle production and of common intelligence support functions. Strengthen the role and performance of the Defense Intelligence Agency (DIA) as a Combat Support Agency and improve the quality of the defense intelligence product through streamlining and reconfiguring DIA to improve its estimative intelligence; strengthening DIA's management of intelligence production and analysis; taking appropriate manpower management steps to ensure a strong military focus within DIA; and assigning DIA the responsibility to perform/oversee basic encyclopedic data base production.

- Ensure an independent intelligence input in the acquisition process by establishing within DIA a capability to validate threat information, to include the target data base, and the procedures the DOD Component intelligence commands or agencies will use in preparing system threat reports for Acquisition Category (ACAT) I, II, III, and IV acquisition programs, and for highly-sensitive classified programs.
- Strengthen the counterintelligence (CI) functions of the Department of Defense through the consolidation of counterintelligence and security activities with existing OASD (C3I) intelligence, security countermeasures and telecommunications, and information system security activities.
- Improve support to OSD through establishment within DIA of a Policy Issues Office, capable of obtaining tailored information and support across the intelligence community, with primary responsibility for focused response to OSD-generated intelligence questions and issues.
- Improve DOD's ability to provide centralized resource management and improve the integration of national and tactical intelligence, including Tactical Intelligence and Related Activities (TIARA), through focusing of OASD (C3I) staff responsibility for planning, policy development, congressional interface, functional management, and budgeting by consolidating existing OSD and General Defense Intelligence Program (GDIP) management, centralizing Defense-wide intelligence policy and resource management; establishing an Intelligence Program Support Group

(IPSG), renamed in FY96 the C4I Integration Support Activity, to consolidate the review of national and tactical programs, develop a DOD-wide architecture, and assess customer satisfaction; and transferring responsibility for the (GDIP) management to the OASD(C3I).

- Restructure and refocus the use of Reserve and National Guard resources to improve support to Defense Intelligence during contingencies through establishment within the OASD (C3I) of a management focus for the use of intelligence reserves and reserve intelligence production, and by tasking the Services and Agencies to develop specific plans for the use of these reserve resources in contingency situations.

Defense Intelligence organization under this plan is graphically shown in Figure 18-2.

Defense Intelligence Agency (DIA).

The Director, DIA is responsible for satisfying the foreign military requirements (less cryptologic) of the SECDEF, OSD, CJCS, OJCS, Joint Staff, CINCs, major DOD components, and other US Government agencies, allied governments, and coalition partners (when required), and has been designated by the CJCS as a DOD *Combat Support Agency*. DIA provides defense intelligence contributions to national intelligence estimates and production capabilities. The Director, DIA is a member of the National Foreign Intelligence Council (NFIC) and is the DCI's executive agent for MASINT as well as the DOD MASINT collection manager. DIA produces, or through tasking and coordination, ensures the production of foreign military and military-related intelligence. The Director, DIA works extensively with the Services to provide support that meets a wide variety of needs. To provide daily support to the Unified Commands and U.S. Forces Korea, NATO, and SHAPE, DIA initiated on-site liaison elements managed by an experienced senior civilian intelligence officer. These liaison elements, called Defense Intelligence Support Offices (ISO), expedite actions and communications between and among the Agency and the commands. To provide tailored support to a Joint Force Commander, DIA can deploy National Intelligence Support Teams (NIST) composed of DIA, NSA, and CIA personnel as well as personnel from other organizations, as required. The NIST deploys with its organic support capability and provides critical on-site intelligence connectivity between the supported command and Washington to ensure receipt of national-level intelligence. Cooperative Service efforts go into the GDIP and the Joint Military Intelligence Program (JMIP), providing a broad range of recommendations to improve future intelligence capabilities. DIA also shares or provides intelligence support to the President, National Security Council Staff, National Warning Staff (NWS), Departments of Energy/State/ Treasury/ and Commerce, and the National Imagery and Mapping Agency (NIMA). The Agency provides central management for the Defense Attaché System and operates the Joint Military Intelligence College (JMIC).

The Military Intelligence Board (MIB), chaired by the Director of the DIA and composed of the senior intelligence officers of the U.S. Army, U.S. Air Force, U.S. Navy, and U.S. Marine Corps, advises the Secretary of Defense and Defense agencies on matters pertaining to military

intelligence. The concerns of the Unified Commands are represented by DIA's Directorate for Intelligence which functions as the J2, Joint Staff. The MIB is the most senior corporate intelligence organization in DOD and advises the SECDEF, CJCS, Military Service Chiefs, CINCs, and Defense agencies on matters pertaining to military intelligence across the broad spectrum of national requirements. The Director DIA seeks consensus across the intelligence community through the MIB process.

The DIA supervises the DOD Indication and Warning System and provides support to the National Military Command Center through the National Military Joint Intelligence Center. The DIA has the responsibility to satisfy the DOD intelligence collection requirements; to coordinate and review activities of the DOD collection resources not assigned to the DIA; and to operate the Defense HUMINT Service (DHS).

National Imagery and Mapping Agency (NIMA).

The NIMA was established on 1 October 1996 to consolidate to the extent practicable all functions of the Defense Mapping Agency. These include defense mapping, charting, and geodetic operations; production, source data storage and retrieval, and management of distribution facilities; and supervision of the Hydrographics/Topographic Center and the Defense Mapping School. NIMA also incorporated all functions of the Central Imagery Office (CIO). NIMA develops and makes recommendations on national imagery policy and is chartered to ensure responsive imagery support to the DOD, the Central Intelligence Agency, and other Federal Government departments. The NIMA tasks and evaluates imagery elements of the DOD in meeting national intelligence requirements and ensures imagery systems are exercised to support military forces. Within the DOD, the NIMA establishes the architectures for imagery tasking, collection, processing, exploitation, and dissemination. The NIMA has responsibility for establishing standards for imagery systems for which the DOD has responsibility, and ensures compatibility and interoperability of these systems. Standards for training of personnel performing imagery tasking, collection, processing, exploitation, and dissemination functions are established by the NIMA. The NIMA also supports and conducts research and development activities related to this imagery function. The NIMA serves as the functional manager for the Consolidated Imagery Program within the National Foreign Intelligence Program and for the Tactical Imagery Program (Tactical Intelligence and Related Activities). The Secretary of Defense and the Director of Central Intelligence are advised by the NIMA on future needs for imagery systems.

National Security Agency (NSA) and Central Security Service (CSS).

The Director of the NSA is also the Chief of the Central Security Service and manages the largest single program in the National Foreign Intelligence Program. He is responsible for the operations of an effective unified organization for SIGINT activity. This responsibility requires extensive interaction, coordination, and cooperation with the Services and other national intelligence agencies. No other department or agency may engage in such activity without a delegation of authority by SECDEF. NSA's SIGINT activities are extremely sensitive and are normally

handled in special channels available to specifically designated personnel in direct support of military commanders, operations, and national foreign intelligence collection requirements. The NSA's SIGINT collection, processing, and dissemination activities involve both positive and counterintelligence information and are in direct support of military commanders and military operations and responsive to national foreign intelligence requirements. The Director of the NSA is responsible for the research and development required to meet the needs for SIGINT and Communications Security (COMSEC). He is the executive agent for executing the responsibilities of the SECDEF for the COMSEC of the Government. He also has oversight of the Defense Cryptologic Program (DCP) that lies outside the National Foreign Intelligence Program, and is responsible for providing cryptologic training and training support to the Services.

In addition, NSA has been given the additional mission of Information Security (INFOSEC) which, in turn, has two components—Communications Security (COMSEC) and Computer Security (COMPUSEC).

Defense Security Service (DSS).

The Defense Investigative Service (DIS) was established in 1972 to consolidate all DOD personnel security investigations and industrial security oversight within one agency and thereby reduce resource requirements, increase managerial efficiency, and provide a more prompt response to overall defense needs for personnel security investigations. As a result of the recent Defense Reform Initiative, the DIS has been renamed the Defense Security Service (DSS) to reflect its broader security mission within the Department of Defense. The new DSS includes the DOD Polygraph Institute, the Personnel Security Research Center and the DOD Security Institute.

ARMY INTELLIGENCE

The Secretary of the Army has delegated to the Under Secretary of the Army responsibility for the general supervision of the intelligence, counterintelligence, investigative, and intelligence oversight activities of the Army. See Figure 18-3 for a simplified organization of the Army Intelligence System.

The intelligence and counterintelligence elements of the military Services are responsible for the planning, direction, collection, processing, and dissemination of military and military-related intelligence, including information on indications and warnings, foreign capabilities, plans and weapons systems, and scientific and technical developments. The conduct of counterintelligence activities and the production and dissemination of counterintelligence studies and reports is a Service responsibility as are the development, procurement, and management of tactical intelligence systems and equipment; the conduct of related research, development, and test and evaluation activities; the development of intelligence doctrine; and the training of intelligence personnel.

Deputy Chief of Staff for Intelligence (DCSINT).

The DCSINT is the senior intelligence officer in the U.S. Army and is responsible to the Chief of Staff for the policy formulation, planning, programming and budgeting (shared with the Deputy Chief of Staff for Operations and Plans (DCSOPS)

ARMY INTELLIGENCE ORGANIZATION

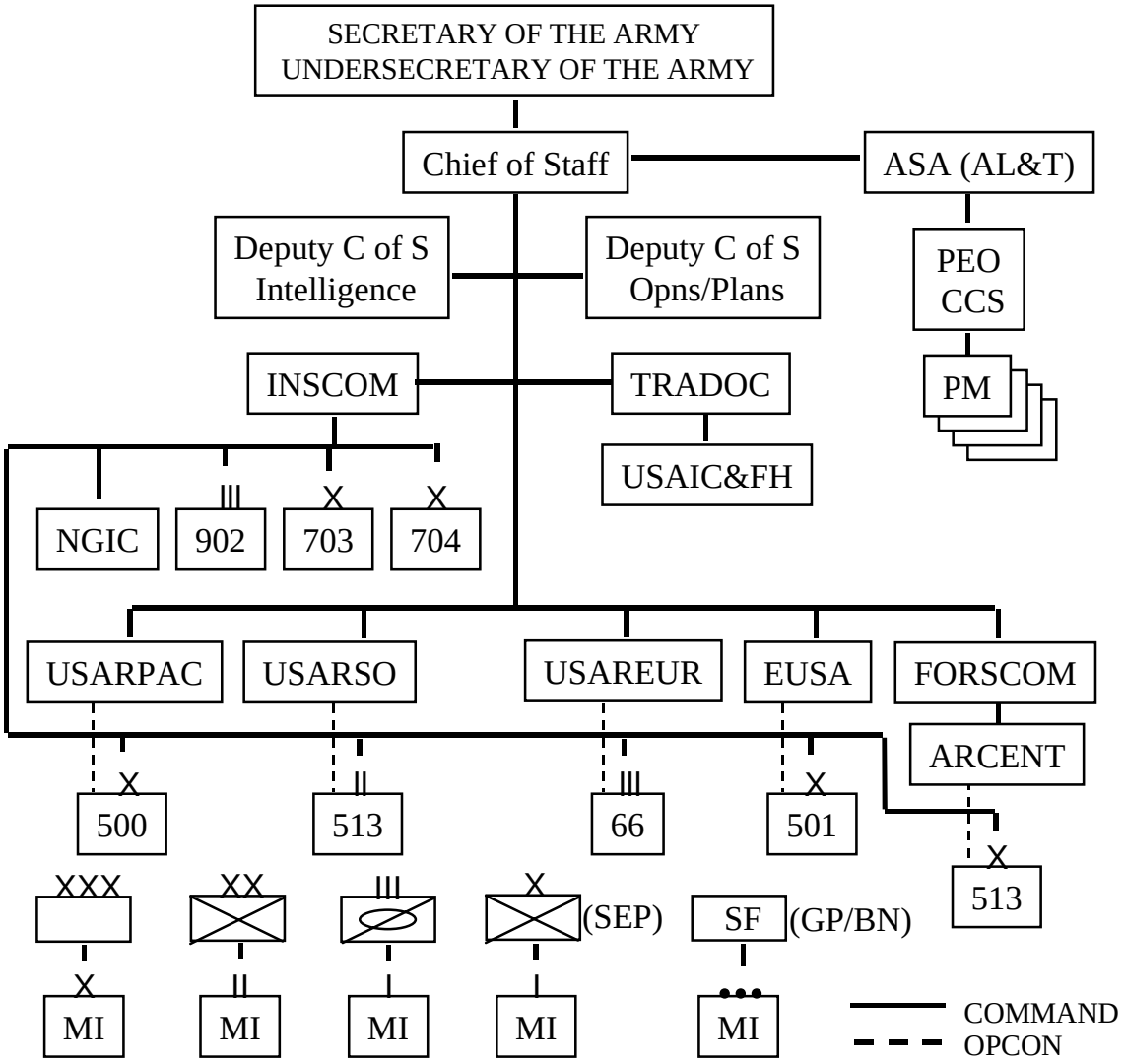

Figure 18-3

for TIARA programs), management, propriety and overall coordination of the intelligence and counterintelligence activities of the Army. The DCSINT has general staff responsibility for intelligence, counterintelligence, intelligence automation, signals intelligence, imagery intelligence, measurement and signature intelligence, censorship, threat validation, intelligence collection, security, meteorological, topographic, and space activities; and monitors Army intelligence training, force structure, and readiness for both the Active and Reserve Components. The DCSINT, under the general guidance and tasking of DIA, exercises general staff supervision over Army and Army-supported Intelligence Data Handling System resources and over all-source intelligence production within the Army; is the Director for Army Budget Program 3I (Intelligence); and is responsible for the Army's input into the DOD Consolidated Cryptologic Program (CCP); the General Defense Intelligence Program

(GDIP); the Foreign Counterintelligence Program (FCIP); and the Army Security and Intelligence Activities Program (S&IA); and is the Army SIGINT focal point. The DCSINT participates in Army POM building by providing advice to Senior Program Managers on ranking of intelligence requirements. Moreover, the DCSINT coordinates top intelligence requirements with MACOMs during submission of POM Assessment.

The DCSINT also shares management, in the Department of the Army, with the DCSPER for the Civilian Intelligence Personnel Management System (CIPMS). CIPMS is a tri-Service, Excepted Service personnel management system for the management of intelligence and intelligence-related civilian personnel in the Army, Navy, and Air Force.

The baseline document for the management of IEW within the Army is the Army Intelligence Master Plan (AIMP). The AIMP is a requirements-based, threat- and technology-driven, comprehensive developmental strategy for the future. It is not, per se, constrained by fiscal or force structure resources. The AIMP, supported by the ASA (RDA)-developed IEW Program Plan for the research, development, and acquisition of IEW systems, provides the basis for the development of the force structure and the fiscally-constrained IEW Chapter of the Army Modernization Plan (AMP) by the DCSOPS, DA. The IEW Chapter of the AMP implements the Army's force modernization principles and is the key planning document in providing long-term continuity of effort within the IEW functional area.

The General Counsel and The Inspector General share responsibility for the oversight of intelligence activities within the Army.

Intelligence and Security Command (INSCOM).

INSCOM, currently a Major Army Command, provides a single commander for those Intelligence and Electronic Warfare (IEW) units which operate at Echelons above Corps (EAC). INSCOM units, which are located both in CONUS and at many overseas locations, support requirements which cross the operational continuum. The operations of INSCOM units include: planning and direction, collection, processing, production and dissemination of all-source, multi-discipline intelligence. In each major overseas area, a Military Intelligence (MI) Brigade or Group provides multi-disciplined IEW support to Army EAC and joint commanders in theater, reinforces MI units organic to operational and tactical commands at the Echelon Corps and Below (ECB), and satisfies tasking from national and departmental authorities for SIGINT, IMINT, TECHINT, MASINT, tactical HUMINT, and counterintelligence operations in response to strategic, operational, and tactical requirements. These activities are being pursued through a multidisciplined force projection brigade concept. In CONUS, single and multi-discipline INSCOM MI brigade units and other organizations, some of them strategically deployable for contingencies, provide a wide range of collection capabilities as well as threat analysis, security, and OPSEC support to national and departmental agencies, contractors for sensitive projects and systems, and CONUS-based tactical consumers, including FORSCOM units and the Army component of United States Central Command. INSCOM also plays a significant role in training at the National Training Center and with its REDTRAIN program which supports maintenance and development of

intelligence skills in EAC and ECB MI units. Finally, INSCOM supports TRADOC in the EAC IEW combat-development process with doctrinal and force structure input, and is a materiel developer for certain specialized types of intelligence-related materiel.

U.S. Army National Ground Intelligence Center (NGIC).

The National Ground Intelligence Center (NGIC), subordinated to INSCOM, is located in Charlottesville, Virginia, with elements at the Navy Yard, Washington, D.C.; Fort Meade, Maryland; and Aberdeen Proving Ground, Maryland. As the Army's Production Center for the DOD IPP community, the NGIC provides basic ground intelligence to U.S. Government Agencies and decision makers. NGIC produces all-source scientific, technical, and general military intelligence on foreign ground forces capabilities and systems in support of Army Title 10 requirements. This intelligence supports customers at all echelons, including Army and DOD force planners, wargamers, doctrinal developers, force modernizers, warfighters and theater joint intelligence centers with a wide range of futures-oriented threat assessments. Key products and production programs include order-of-battle and tables of organization and equipment for foreign ground forces, projection out 20 years; detailed assessments of future threats tactical/operational capabilities; conflict scenarios; and forecast of future regions of conflict of interest to US force planners; and provides threat documentation for Army R&D and procurement programs. These products and programs require collection (MASINT and Multi-Disciplinary collection); all-source analysis, production integration; and requirements management.

Information Operations (IO).

Information Warfare/Command and Control Warfare (IW/C2W), a field that has increased in significance as a result of lessons learned during the Gulf War, applies to a wide range of plans and actions designed to afford the United States and coalition forces a decisive information advantage across the full spectrum of military operations. The capability to execute IW/C2W places an increased demand on intelligence to rapidly and accurately identify both friendly and enemy vulnerabilities. Although IO is an operations function, intelligence is an integral part of the IW/C2W planning and execution actions that will degrade an adversary's use of information while protecting those of friendly forces.

Information Operations is the Army and Marine Corps doctrine that implements Information Warfare through continuous military actions that enable, enhance, and protect the commander's decision cycle while degrading that of the enemy to achieve an information advantage. An information advantage can be exploited to enable the commander to operate within the enemy's decision cycle. Command and Control Warfare (C2W), comprising C2-Attack and C2-Protect, is the Army's principal means of conducting Information Operations. Intelligence acquires, manages, and uses information to identify enemy C2W weaknesses for possible exploitation. Counterintelligence concentrates on finding friendly C2 weaknesses that may be exploited by an enemy force. Supporting C2-Attack and C2-Protect requires that both intelligence and counterintelligence remain abreast of current and emerging command and control technology in both the commercial and military arenas.

In FY95, the Army organized and activated the Land Information Warfare Activity (LIWA) within the Intelligence and Security Command (INSCOM) to assist the Land Component Commander deal with the complexities of Command and Control Warfare planning and execution. Tasked by the DCSOPS, HQDA, the LIWA is patterned after the Joint Command and Control Warfare Center (JC2WC) to deploy tailored field support teams (FST) to specific land component commands during exercises, contingency planning, and operations. LIWA provides technical expertise and operational connectivity with other organizations and agencies supporting C2W operations.

Commanders use IEW support to anticipate the battle, understand the battlefield, and influence the outcome of operations. The preeminent function of Army Intelligence is to support the tactical commanders decisionmaking process. The tactical commander drives the Army intelligence effort; the ACofS, G2/S2, is the individual responsible for planning and directing, collecting, processing, producing, and disseminating intelligence within the command. At corps, division, ACR/separate brigade, and Special Operations Forces group/battalion, a MI unit is organic to the command, as shown in Figure 18-3. The MI unit commander provides the G2/S2 with the resources to accomplish the intelligence mission by training, maintaining, and employing the organic intelligence assets of the command. Additional assets leverage national, theater, Sister Service, and other intelligence systems to provide intelligence to the tactical commanders at all echelons. *FM 34-1: IEW Operations*, the keystone intelligence manual, expands upon *FM 100-5: Operations*, and provides detail on the doctrinal foundations for IEW operations and the employment of tactical MI units.

Reserve Component (RC) Support.

The Reserve Components (RC) participate with Active Component (AC) MI units at all echelons and are involved in virtually every aspect of military intelligence operations. In certain areas, USAR and National Guard MI capabilities, i.e. scientific & technical analysis, political-military estimates, substantive basic intelligence, are equal to, or even exceed, those in the active force. This phenomenon can be attributable to the fact that many MI reservists, officer and enlisted, are professional civilian intelligence employees of the national intelligence and reconnaissance agencies, the Services' intelligence departments and agencies, federally funded research centers, colleges and universities, and other US Government departments performing similar activities. Consequently, their exposure to, and involvement in, intelligence operations on a daily basis rivals their uniformed counterparts. The RC's contributions to filling the Army's linguist requirements are critical. The RC MI force is in the process of increasing its capacity for timely response to intelligence production requirements. RC MI centers across the country are being connected to DOD telecommunications networks. This connectivity allows RC MI units and soldiers to receive tasks from Active Component (AC) intelligence organizations, perform research and analysis within DOD data bases, and file production reports back to the AC organization—all within a relatively short time. RC MI is moving rapidly to a force architecture that will integrate it more fully into the operational capabilities of the AC, making the Reserve Components an increasingly valuable partner.

Resource Management.

The primary means for resource management within the intelligence community is the National Foreign Intelligence Program. It includes the programs of the CIA, certain intelligence programs of the DOD, and other programs of agencies designated by the DCI, a department head, or by the President as constituting the National Foreign Intelligence Program (NFIP). The DCI has authority for approval of the NFIP budget submitted to the President through the OMB, and must present and justify the budget to the Congress. The DCI provides guidance for program and budget development to program managers and heads of departments and agencies. The Executive Director for Intel Community Affairs is the principal adviser to the DCI on all matters relating to the NFIP budget prior to its presentation to the President and Congress.

The Army participates in three of the programs of the NFIP: the Consolidated Cryptologic Program (CCP), the Foreign Counterintelligence Program (FCIP) and the General Defense Intelligence Program (GDIP). The Program Manager for the CCP is the Director, National Security Agency. The CCP includes resources for SIGINT projects and activities. The Director DIA is the program manager for the GDIP, and funds collection, production and infrastructure which includes funds for DIA, Technical Reconnaissance (MASINT), some intelligence activities of the unified commands, and the FCIP, which provides resources for some CI activities. DOD FCIP Program Manager is Director of CI and Security, OASD (C3I). Program and budget information is prepared by each of the Services and is forwarded through program managers to the DCI.

In addition to the NFIP budget, many intelligence resources are included in the DOD Tactical Intelligence and Related Activities (TIARA) program. This program includes most intelligence resources directly supporting operational commanders.

Unified Commanders formally participate in the Planning, Programming, and Budgeting System (PPBS) process for intelligence resources. Through the Command Intelligence Architecture Program (CIAP), Unified Commanders identify their intelligence collection, processing, and dissemination resource requirements. The CIAP has become the driving force for acquiring the requisite military intelligence capabilities through the 1990s.

Collection Management.

The intelligence cycle begins and ends with the consumer. A consumer's requirements are passed to the producer for fulfillment. If the producer cannot satisfy the consumer's requirements, the producer levies the requirement on the collector. The user must be able to state clearly his intelligence interests or needs (requirements) in addition to those that are already satisfied by existing finished intelligence. Requirements compete for limited collection resources at the national, departmental, strategic, operational, and tactical levels. Requirements are prioritized in accordance with the Intelligence Priorities for Strategic Planning (IPSP). The military commander must make his case for the priority of his requirement if resources not assigned or organic to his command are needed to fulfill the requirement.

The DIA, in its support role to the JCS, prepares a listing of intelligence priorities for strategic planning for JCS publication and validates the intelligence

requirements of the military Services. A prioritized list of both long-term and short-term national interests is established by the NSC and passed to the CIA. There a determination is made as to whether sufficient intelligence exists to fulfill the requirement or whether additional intelligence is needed. If it is, detailed prioritized requirements are passed to the DCI's Community Management Staff (CMS) for collection tasking.

All collection operations are conducted in response to validated requirements for the production of finished intelligence. The CMS tasks its members for collection to fulfill prioritized requirements. The selection of the specific collection resource rests with the department or the program manager. The management aspects of collection involve ensuring that the assets selected are the most cost-effective that can fulfill the requirement on a timely basis.

Collection operations tasked by the DIA in response to DOD-generated requirements are normally conducted on an all-source, common-service basis. Conduct of intelligence operations at the tactical level to directly support the commander's immediate needs is usually accomplished by assigned or supporting intelligence organizations. Tactical commanders obtain most information on their areas of operation from assigned or supporting assets including MI units, artillery, cavalry, aviation, and maneuver units in contact. Tactical commanders leverage national capabilities by placing small numbers of tactical force intelligence soldiers at key nodes in the intelligence system to provide direct response to supported commanders' requirements. Additional information and intelligence on the area of interest is provided from higher echelons.

Analysis and Production Management.

National intelligence production is the responsibility of the DCI and is exercised through the CIA's Directorate of Intelligence, which establishes schedules and priorities for all national intelligence production. Further, the directorate retains the resources and capability to produce intelligence assessments which are not coordinated with other elements of the Intelligence Community.

The Deputy to the DCI for National Intelligence is the principal adviser to the DCI on the production of national intelligence, both as to the manner in which it is accomplished and what it contains. He is responsible for organizing national efforts to assess and evaluate foreign intelligence data in support of intelligence objectives established by the NSC. He is the head of the Directorate of Intelligence and oversees production generated in response to standing requirements, new requirements, or as the need is perceived.

No single intelligence product format meets the needs of all consumers. It is necessary to have a continuing dialogue between the consumer and the producer of intelligence while assuring that the consumer does not influence the conclusions of the final product.

The most prestigious intelligence product is the President's Daily Brief (PDB), which is prepared by the Directorate of Intelligence for DCI approval and forwarding to the President. The PDB may be considered as the DCI's principal daily report to the President. Other national reports include the National Intelligence Brief and the Military Intelligence Digest. National Intelligence Estimates and similar publications are reviewed by the NFIB prior to submission to the DCI for approval and subsequent dissemination.

Individual departments and agencies establish their own production schedules and priorities for the production of departmental intelligence. The DIA establishes production schedules in the DOD and distributes responsibilities among the unified and specified commands.

DIA's Directorate for Intelligence Production (DI), formerly called the National Military Intelligence Production Center (NMIPC), produces, or manages the production of, all-source military intelligence to support the policy, planning, and operational requirements of OSD, JCS, the Services, and the Unified Commands. As the DOD Production Functional Manager, DI ensures that DOD intelligence production requirements are articulated; resources are programmed and executed in compliance with national and DOD guidance; and programs are re-evaluated as missions, technical capabilities, and threat environment change.

SUMMARY

Intelligence is vital to the national security of the United States, but the importance of intelligence in various program and planning areas is not always fully recognized. Resources should be used as efficiently as possible, but concentration should be on intelligence production.

The National Foreign Intelligence Program, under the supervision of the DCI, includes CIA programs, major DOD programs, and programs within other U.S. Government agencies. The National Foreign Intelligence Program provides overall review, guidance, and direction for all national foreign intelligence and counterintelligence activities.

LIST OF REFERENCES

(1) The President. "United States Intelligence Activities." *Executive Order 12333,* 4 December 1981.

(2) U.S. Department of Defense. *DOD Directive TS-3600.1: Information Warfare,* 21 December 1993.

(3) U.S. Department of Defense. *DOD Directive 5105.21: Defense Intelligence Agency.*

(4) U.S. Department of Defense. *DOD Directive 5105.56: Central Imagery Office,* 6 May 1992.

(5) U.S. Department of Defense. *DOD Directive 5240.1-R: Procedures Governing the Activities of DOD Components That Affect U.S. Persons.*

(6) *DOD Pam 0000-151C2-95, Department of Defense Intelligence Production Program*, May 1995.

(7) Joint Publication 2-02, *National Intelligence Support to Joint Operations.*

(8) DIA Pam *National Military Intelligence Production Center*, Jan 1996.

(9) DIA Pub *Vector 21: A Strategic Plan For The Defense Intelligence Agency*, 1996

(10) DIA, Joint Military Intelligence Training Center, *An Intelligence Resource Manager's Guide*, 1994 Edition.

(11) *Director of Central Intelligence Directive (DCID) 2/9:Management of National Imagery Intelligence*, effective 1 June 1992.

(12) CIA Pub *A Consumer's Guide To Intelligence*, PAS 95-00010, July 1995.

(13) U.S. Department of the Army. *Army Regulation 381-10: U.S. Army Intelligence Activities,* 1 July 1984.

(14) U.S. Department of the Army. *Army Regulation 380-19: Information Systems Security*, 27 February 1998.

(15) U.S. Department of the Army. *Field Manual 34-1: Intelligence and Electronic Warfare Operations,* 27 September 1994.

(16) U.S. Department of the Army. *Field Manual 34-8: Combat Commander's Handbook on Intelligence,* 28 September 1992.
(17) *TRADOC Pam 525-5: Force XXI Operations,* 1 August 1994.
(18) *TRADOC Pam 525-69*: *Concept for Information Operations,* 1 August 1995.
(19) *TRADOC Pam 525-75: Intel XXI-A concept for Force XXI Intelligence Operations,* 1 November 1996.